UNCLASSIFIED

Microsoft IE Version 6

Version: 4

Release: 2

23 April 2010

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-3427
Group Title: IE - Zones: Use Only Machine Settings
Rule ID: SV-3427r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI320
Rule Title: Internet Explorer is not configured to require consistent security zone settings to all users.

Vulnerability Discussion: This setting enforces consistent security zone settings to all users of the computer. Security Zones control browser behavior at various web sites and it is desirable to maintain a consistent policy for all users of a machine.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_HKLM_only

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Use only machine settings" to "Enabled".

Group ID (Vulid): V-3428
Group Title: IE - Zones: Do Not Allow Users to Change Policies
Rule ID: SV-3428r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI319
Rule Title: Internet Explorer is configured to Allow Users to Change Policies.

Vulnerability Discussion: This setting prevents users from changing the Internet Explorer policies on the machine. Policy changes should be made by Administrators only, so this setting should be Enabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_Options_Edit

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Do Not Allow Users to Change Policies" to "Enabled".

Group ID (Vulid): V-3429
Group Title: IE - Zones: Do Not Allow Users to Add/Delete Sites
Rule ID: SV-3429r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI318
Rule Title: Internet Explorer is configured to Allow Users to Add/Delete Sites.

Vulnerability Discussion: This setting prevents users from adding sites to various security zones. Users should not be able to add sites to different zones, as this could allow them to bypass security controls of the system.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Value Name: Security_Zones_Map_Edit

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Security Zones: Do Not Allow Users to Add/Delete Sites" to "Enabled".

Group ID (Vulid): V-3430
Group Title: IE - Make Proxy Settings Per Machine
Rule ID: SV-3430r10_rule
Severity: CAT III
Rule Version (STIG-ID): DTBI367
Rule Title: Internet Explorer is not configured to disable making Proxy Settings Per Machine.

Vulnerability Discussion: This setting controls whether or not the Internet Explorer proxy settings are configured on a per-user or per-machine basis.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Make proxy settings per-machine (rather than per user)" to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Criteria: If the value ProxySettingsPerUser is REG_DWORD = 1, this is not a finding.

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Make proxy settings per-machine (rather than per user)" to "Disabled".

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\

Criteria: Set the value ProxySettingsPerUser to REG_DWORD = 1.

Group ID (Vulid): V-3431
Group Title: IE - Disable Automatic Install of IE Components
Rule ID: SV-3431r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI316
Rule Title: Internet Explorer is configured to allow Automatic Install of components.

Vulnerability Discussion: This setting controls the ability of Internet Explorer to automatically install components if it goes to a site that requires components that are not currently installed. The System Administrator should install all components on the system. If additional components are necessary, the user should inform the SA and have the SA install the components.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Internet Explorer\InfoDelivery\Restrictions\

Value Name: NoJITSetup

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Disable Automatic Install of Internet Explorer components" to "Enabled".

Group ID (Vulid): V-3432
Group Title: IE - Disable Periodic Check for IE Updates
Rule ID: SV-3432r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI317
Rule Title: Internet Explorer is configured to automatically check for updates.

Vulnerability Discussion: This setting determines whether or not Internet Explorer will periodically check the Microsoft web sites to determine if there are updates to Internet Explorer available. The SA should manually install all updates on a system so that configuration control is maintained.

Responsibility: System Administrator
IAControls: DCSL-1

Check Content:
If the following registry value doesn't exist or is not configured as specified, this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Policies\Microsoft\Internet Explorer\InfoDelivery\Restrictions\

Value Name: NoUpdateCheck

Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer "Disable Periodic Check for Internet Explorer Software Updates" to "Enabled".

Group ID (Vulid): V-3433
Group Title: IE - Disable Software Update Shell Notifications
Rule ID: SV-3433r9_rule
Severity: CAT III
Rule Version (STIG-ID): DTBI137
Rule Title: Internet Explorer is configured to notify users when programs are modified through the software distribution channel.

Vulnerability Discussion: Microsoft Internet Explorer now supports a software distribution channel that may be used to update software installed on a machine. If this setting is enabled, users will not be notified when programs are modified through the software distribution channel. This allows administrators to update workstations without user intervention.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
If the following registry value exists and its value is not set to 1, then this is a finding:

Registry Hive: HKEY_LOCAL_MACHINE
Subkey: \Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
Value Name: NoMSAppLogo5ChannelNotify
Type: REG_DWORD
Value: 1

Fix Text: Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer “Disable Software Update Shell Notifications on Program Launch” to “Enabled”.

Group ID (Vulid): V-6227
Group Title: DTBG003-Installed version of IE is unsupported
Rule ID: SV-6277r6_rule
Severity: CAT I
Rule Version (STIG-ID): DTBG003
Rule Title: The installed version of IE is at an unsupported version.

Vulnerability Discussion: Unsupported versions are no longer being evaluated or updated for security related issues.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Search for the shdocvw.dll file using the Start menu “Search | For Files or Folders…” facility. Determine the version of the shdocvw.dll file.

Criteria: If the version number of the shdocvw.dll file is not 6.00.x.y or greater, then this is a Finding.

Fix Text: Upgrade to the supported software version.

Group ID (Vulid): V-6228
Group Title: DTBI001 - The IE home page is not set correctly
Rule ID: SV-6278r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI001
Rule Title: The IE home page is not set to blank, a local file, or a trusted site.

Vulnerability Discussion: By setting this parameter appropriately, a malicious web site will be automatically loaded into a browser which may contain mobile code.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\InternetExplorer\Main

Criteria: If the value StartPage is about:blank or a trusted site or a local file, this is not a finding.

Fix Text: Change StartPage value to about:blank, a trusted site, or a local file.

Group ID (Vulid): V-6229
Group Title: DTBI002 - IE Local zone parameter is set incorrect
Rule ID: SV-6279r6_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI002
Rule Title: IE Local zone security parameter is set incorrectly.

Vulnerability Discussion: The Local zone must be set to custom level so the other required settings for the zone can take effect.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value Currrentlevel is 0, this is not a finding.

Fix Text: Change the value of registry HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1 to Currentlevel is 0

Group ID (Vulid): V-6230
Group Title: DTBI003-IE Trusted zone parameter is set incorrect
Rule ID: SV-6280r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI003
Rule Title: The IE Trusted sites zone security parameter is set incorrectly.

Vulnerability Discussion: The Trusted sites zone must be set to custom level so the other required settings for the zone can take effect.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value Currrentlevel is 0, this is not a finding.

Fix Text: Change value of registry HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2 to Currentlevel is 0

Group ID (Vulid): V-6231
Group Title: DTBI004-IE Internet zone parameter is set incorrec
Rule ID: SV-6281r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI004
Rule Title: The IE Internet zone security parameter is set incorrectly.

Vulnerability Discussion: The Internet zone must be set to custom level so the other required settings for the zone can take effect.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value Currrentlevel is 0, this is not a finding.

Fix Text: Change the value of registry HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3 to Currentlevel is 0.

Group ID (Vulid): V-6232
Group Title: DTBI005-IE Restricted zone parameter is set incorr
Rule ID: SV-6282r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI005
Rule Title: The IE Restricted sites zone security parameter is set incorrectly.

Vulnerability Discussion: The Restricted sites zone must be set to custom level so the other required settings for the zone can take effect.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value Currrentlevel is 0, this is not a finding.

Fix Text: Change the value of registry HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 to Currentlevel is 0.

Group ID (Vulid): V-6233
Group Title: DTBI006-IE Local zone includes parameter not set
Rule ID: SV-6283r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI006
Rule Title: The IE Local zone includes parameter is not set correctly.

Vulnerability Discussion: This parameter controls which sites are by default in the local zone. Since this is the least restrictive zone these settings ensure that sites are not included in this zone by default.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value Flags is less than or equal to 0x43 (hex) or 67 (Dec), this is not a finding.

Fix Text: Change the value of registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1 to Flags is 0x43.

Group ID (Vulid): V-6234
Group Title: DTBI007-IE third party cookies not set correctly
Rule ID: SV-6284r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI007
Rule Title: The IE third party cookies parameter is not set correctly.

Vulnerability Discussion: This parameter ensures that third party cookies are blocked. Third party cookies come from a site other than the site being browsed. Since these cross sites, the storing unwanted data or allowing data to be retrieved later via the cookie is of greater concern for malicious activity.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: From the Tools/Internet Options dialog, Select the Privacy tab and click the Advanced button.

Criteria: If the Third-party Cookies are not configured to Block, this is a finding.

Fix Text: Under Tools/Internet Options, select the Privacy Tab and click the Advanced button. Change third party cookies to blocked.

Group ID (Vulid): V-6236
Group Title: DTBI012-IE signature checking is not set correctly
Rule ID: SV-6286r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI012
Rule Title: The IE signature checking parameter is not set correctly.

Vulnerability Discussion: This parameter will ensure digital signatures are checked on downloaded programs.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Microsoft\ Internet Explorer\Download

Criteria: If the value CheckExeSignatures is yes, this is not a finding.

Fix Text: Change the value of registry key HKCU\Software\Microsoft\ Internet Explorer\Download to CheckExeSignatures is yes.

Group ID (Vulid): V-6237

Group Title: DTBI013-IE save encrypted pages to disk is not set
Rule ID: SV-6287r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI013
Rule Title: The IE save encrypted pages to disk parameter is not set correctly.

Vulnerability Discussion: This parameter ensures pages using SSL or TLS are not cached to the local drive. This ensures sensitive data from a web site does not remain on the machine that is not properly protected.

Potential Impacts:
This will cause the browser's back button to not work for pages that use SSL or TLS.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value DisableCachingOfSSLPages is 1, this is not a finding.
If the Do not save encrypted pages to disk is 0 enabled and the permissions of the Temporary Internet files folder are not the same as, or more restrictive than, those in the following table, this is a Finding.

variable\Temporary Internet Files(The variable portion of the path name depends on the configuration setting in Internet Explorer.)
Administrators ALL
CREATOR OWNER ALL
SYSTEM ALL
[user] ALL

Fix Text: Change the value of registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings to DisableCachingOfSSLPages is 1

Group ID (Vulid): V-6238
Group Title: DTBI014-IE SSL/TLS parameter is not set correctly
Rule ID: SV-6288r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI014
Rule Title: The IE SSL/TLS parameter is not set correctly.

Vulnerability Discussion: This parameter ensures SSL and TLS are able to be used from the browser.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value SecureProtocols value is A8 or A0, this is not a finding.

Fix Text: Change registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings so that value SecureProtocols value is A8 or A0.

Group ID (Vulid): V-6239
Group Title: DTBI015-IE warning of invalid certificates not set
Rule ID: SV-6289r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI015
Rule Title: The IE warning of invalid certificates parameter is not set correctly

Vulnerability Discussion: This parameter warns users if the certifcate being presented by the web site is invalid. Since server certificates are used to validate the identity of the web server it is critical to warn the user of a potential issue with the certificate being presented by the web server.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value WarnonBadCertRecving value is 1, this is not a finding.

Fix Text: Change the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings to the value WarnonBadCertRecving is 1

Group ID (Vulid): V-6240
Group Title: DTBI016-IE changing zones is not set correctly
Rule ID: SV-6290r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI016
Rule Title: The IE changing zones parameter is not set correctly.

Vulnerability Discussion: This parameter warns the user when changing between zones. This conveys important information to the user so the user is reminded that the zone has changed and the possiblity the type of data to be entered in the site has changed. Also the user expected actions have also changed based upon what happens when a mobile code technology is encountered.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value WarnonZoneCrossing value is 1, this is not a finding.

Fix Text: Change the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings to the value WarnonZoneCrossing is 1.

Group ID (Vulid): V-6241
Group Title: DTBI017-IE form redirect is not set correctly

Rule ID: SV-6291r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI017
Rule Title: The IE form redirect parameter is not set correctly.

Vulnerability Discussion: This parameter warns the user that input from the form is being redirected to another web site. Since the form may contain sensitive data the user must be warned that the data is not being directed to the site the user was using. This enables the user to make a decision if the data on the form is appropriate for inclusion into the new web site.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

Criteria: If the value WarnOnPostRedirect value is 1, this is not a finding.

Fix Text: Change the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings to the value WarnOnPostRedirect is 1.

Group ID (Vulid): V-6242
Group Title: DTBI021-Users can change advanced settings in IE
Rule ID: SV-6292r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI021
Rule Title: Users can change the advanced settings in IE.

Vulnerability Discussion: Since most of the IE settings can be changed through the GUI, it is important to ensure that user's cannot change these settings. Some settings will restrict users from visiting certain sites or will restrict the functionality of sites. It is important that access to changing the settings is removed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel

Criteria: If the value AdvancedTab is 1, this is not a finding. If the value is not 1 or the key is not present, this is a finding.

Fix Text: Change the registry key HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel to the value AdvancedTab is 1.

Group ID (Vulid): V-6243
Group Title: DTBI022-Download signed Active X controls-Internet
Rule ID: SV-6293r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI022

Rule Title: The Download signed ActiveX controls property is not set properly for the Internet Zone.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1001 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria:Set the value 1001 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6244
Group Title: DTBI023-Download unsigned ActiveX controls-Interne
Rule ID: SV-6294r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI023
Rule Title: The Download unsigned ActiveX controls property is not set properly for the Internet Zone.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1004 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1004 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6245
Group Title: DTBI024-Initialize and script ActiveX controls
Rule ID: SV-6295r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI024
Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Internet Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe scripting should not be executed. Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6246
Group Title: DTBI026-Script ActiveX marked safe for scripting
Rule ID: SV-6296r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI026
Rule Title: The Script ActiveX controls marked safe for scripting property is not set properly for the Internet Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1405 is REG_DWORD = 1 (Prompt = 1), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1405 is REG_DWORD = 1 (Prompt = 1).

Group ID (Vulid): V-6248
Group Title: DTBI030-Font download control - Internet Zone
Rule ID: SV-6300r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI030
Rule Title: The Font download control is not set properly for the Internet Zone.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1604 is REG_DWORD = 1 (Prompt = 1), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1604 to REG_DWORD = 1 (Prompt = 1).

Group ID (Vulid): V-6249
Group Title: DTBI031-Java Permissions not set for Internet Zone
Rule ID: SV-6301r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI031
Rule Title: The Java Permissions is not set properly for the Internet Zone.

Vulnerability Discussion: Java must have level of protections based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1C00 is REG_DWORD = 0 (Disabled = 0), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1C00 to REG_DWORD = 0 (Disabled = 0).

Group ID (Vulid): V-6250
Group Title: DTBI032-Access data sources across domains-Interne
Rule ID: SV-6302r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI032
Rule Title: The Access data sources across domains is not set properly for the Internet Zone.

Vulnerability Discussion: Access to data sources across multiple domains must be controlled based upon the site being browsed.

Responsibility: System Administrator

IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1406 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1406 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6251
Group Title: DTBI034-Display mixed content - Internet Zone
Rule ID: SV-6303r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI034
Rule Title: The Display mixed content is not set properly for the Internet Zone.

Vulnerability Discussion: Display mixed content must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1609 is REG_DWORD = 1 (Prompt = 1), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1609 to REG_DWORD = 1 (Prompt = 1).

Group ID (Vulid): V-6252
Group Title: DTBI035-Dont prompt for client certificate-Interne
Rule ID: SV-6304r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI035
Rule Title: The Don't prompt for client certificate selection when no certificate or only one certificate exists is not set properly for the Internet Zone.

Vulnerability Discussion: Client certificates should not be presented to web sites without the user's acknowledgement.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1A04 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1A04 to REG_DWORD=3 (Disabled).

Group ID (Vulid): V-6253
Group Title: DTBI036-Drag and drop or copy and paste-Internet
Rule ID: SV-6305r9_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI036
Rule Title: The Allow Drag and drop or copy and paste files is not set properly for the Internet Zone.

Vulnerability Discussion: Drag and Drop or copy and paste files must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value for 1802 is REG_DWORD = 3 (Disable= 3) or the value does not exist, this is not a finding.

Fix Text: If a value for this zone is present and not set to 3 change the registry key
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1802 to REG_DWORD = 3 (Disable= 3).

Group ID (Vulid): V-6254
Group Title: DTBI037-Installation of desktop items - Internet
Rule ID: SV-6306r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI037
Rule Title: The Installation of desktop items is not set properly for the Internet Zone.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1800 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1800 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6255
Group Title: DTBI038-Launching programs and files in IFRAME-Int
Rule ID: SV-6307r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI038
Rule Title: The Launching programs and files in IFRAME is not set properly for the Internet Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1804 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1804 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6256
Group Title: DTBI039-Navigate sub-frames across domains-Interne
Rule ID: SV-6311r9_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI039
Rule Title: The Navigate sub-frames across different domains is not set properly for the Internet Zone.

Vulnerability Discussion: Frames that navigate across different domains are a security concern because the user may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1607 is REG_DWORD = 1 (Prompt = 1), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1607 to REG_DWORD = 1 (Prompt = 1).

Group ID (Vulid): V-6257
Group Title: DTBI040-Software channel permissions - Internet
Rule ID: SV-6313r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI040
Rule Title: The Software channel permissions is not set properly for the Internet Zone.

Vulnerability Discussion: Software Channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1E05 is REG_DWORD = 65536 (High Safety), this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1E05 to REG_DWORD = 65536 (High Safety).

Group ID (Vulid): V-6258
Group Title: DTBI041-Submit non-encryped form data - Internet
Rule ID: SV-6315r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI041
Rule Title: The Submit non-encrypted form data is not set properly for the Internet Zone.

Vulnerability Discussion: The user needs to be prompted before sending information from a browser that is not encrypted.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1601 is REG_DWORD = 1 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1601 to REG_DWORD = 1 (Prompt).

Group ID (Vulid): V-6259
Group Title: DTBI042-Userdata persistence - Internet Zone
Rule ID: SV-6316r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI042
Rule Title: The Userdata persistence is not set properly for the Internet Zone.

Vulnerability Discussion: Userdata persistence must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1606 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1606 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6260
Group Title: DTBI044-Allow paste operations via script-Internet
Rule ID: SV-6318r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI044
Rule Title: The Allow paste operations via script is not set properly for the Internet Zone.

Vulnerability Discussion: Allow paste operations via script must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1407 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1407 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6261
Group Title: DTBI045-Scripting of Java applets - Internet Zone
Rule ID: SV-6319r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI045
Rule Title: The Scripting of Java applets is not set properly for the Internet Zone.

Vulnerability Discussion: Java Applets must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1402 is REG_DWORD = 1 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1402 to REG_DWORD = 1 (Prompt).

Group ID (Vulid): V-6262
Group Title: DTBI046-User Authentication-Logon - Internet Zone
Rule ID: SV-6321r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI046
Rule Title: The user Authentication - Logon is not set properly for the Internet Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: If the value 1A00 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3

Criteria: Set the value 1A00 to REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6263
Group Title: DTBI052-Download signed ActiveX - Local Zone
Rule ID: SV-6322r6_rule
Severity: CAT II

Rule Version (STIG-ID): DTBI052
Rule Title: The Download signed ActiveX controls property is not set properly for the Local Zone.

Vulnerability Discussion: Active X controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1001 is REG_DWORD 1 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1001 to REG_DWORD 1 (Prompt).

Group ID (Vulid): V-6264
Group Title: DTBI053-Download unsigned ActiveX - Local Zone
Rule ID: SV-6324r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI053
Rule Title: The Download unsigned ActiveX controls property is not set properly for the Local Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1004 is REG_DWORD = 3, this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1004 to REG_DWORD = 3.

Group ID (Vulid): V-6265
Group Title: DTBI054-Initialize and script ActiveX - Local Zone
Rule ID: SV-6325r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI054
Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Local Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a

complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1201 is REG_DWORD 3, this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1201 to REG_DWORD 3.

Group ID (Vulid): V-6266
Group Title: DTBI056-Script ActiveX controls marked safe-Local
Rule ID: SV-6326r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI056
Rule Title: The Script ActiveX controls marked safe for scripting property is not set properly for the Local Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1405 is REG_DWORD 1 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1405 to REG_DWORD 1 (Prompt).

Group ID (Vulid): V-6267
Group Title: DTBI061-Java Permissions not set - Local Zone
Rule ID: SV-6327r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI061
Rule Title: The Java Permissions is not set properly for the Local Zone.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1C00 is REG_DWORD = 65536, (High Safety), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: Set the value 1C00 to REG_DWORD = 65536, (High Safety).

Group ID (Vulid): V-6268
Group Title: DTBI062-Access data sources across domains-Local
Rule ID: SV-6328r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI062
Rule Title: The Access data sources across domains is not set properly for the Local Zone.

Vulnerability Discussion: The user must know when data access crosses sources to ensure the data is being received from a source that is known.

IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1406 is REG_DWORD 1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1406 is REG_DWORD 1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6271
Group Title: DTBI065-Dont prompt client certificate - Local zon
Rule ID: SV-6331r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI065
Rule Title: The Don't prompt for client certificate selection when no certificate or only one certificate exists is not set properly for the Local Zone.

Vulnerability Discussion: Client certificates should not be presented to web sites without the user's acknowledgement.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1A04 is REG_DWORD = 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1A04 is REG_DWORD = 3 (Disabled).

Group ID (Vulid): V-6272
Group Title: DTBI067-Installation of desktop items - Local zone
Rule ID: SV-6333r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI067
Rule Title: The Installation of desktop items is not set properly for the Local Zone.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1800 is REG_DWORD 1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1800 is REG_DWORD 1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6273
Group Title: DTBI068-Launching programs and files in IFRAME-Loc
Rule ID: SV-6334r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI068
Rule Title: The Launching programs and files in IFRAME is not set properly for the Local Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1804 is REG_DWORD 1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1804 is REG_DWORD 1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6274
Group Title: DTBI070-Software channel permissions - Local Zone
Rule ID: SV-6336r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI070
Rule Title: The Software channel permissions is not set properly for the Local Zone.

Vulnerability Discussion: Software channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1E05 is REG_DWORD = 65536 (High Safety), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1E05 is REG_DWORD = 65536 (High Safety).

Group ID (Vulid): V-6275
Group Title: DTBI074-Allow paste operations via script - Local
Rule ID: SV-6337r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI074
Rule Title: The Allow paste operations via script is not set properly for the Local Zone.

Vulnerability Discussion: The Allow paste operations via script must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1407 is REG_DWORD 1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1407 is REG_DWORD 1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6276
Group Title: DTBI076-User Authentication - Logon - Local Zone
Rule ID: SV-6338r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI076
Rule Title: The User Authentication - Logon is not set properly for the Local Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1A00 is REG_DWORD = 0 (Automatically logon with current username and password), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1

Criteria: If the value 1A00 is REG_DWORD = 0 (Automatically logon with current username and password).

Group ID (Vulid): V-6277
Group Title: DTBI082-Download signed ActiveX - Trusted Sites
Rule ID: SV-6339r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI082
Rule Title: The Download signed ActiveX controls property is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1001 is REG_DWORD 1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1001 is REG_DWORD 1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6278
Group Title: DTBI083-Download unsigned ActiveX - Trusted Sites
Rule ID: SV-6340r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI083
Rule Title: The Download unsigned ActiveX controls property is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1004 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1004 is REG_DWORD=3 (Disabled).

Group ID (Vulid): V-6279
Group Title: DTBI084-Initialize and script Activex - Trusted Si
Rule ID: SV-6341r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI084
Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked
safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1201 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1201 is REG_DWORD=3 (Disabled).

Group ID (Vulid): V-6280
Group Title: DTBI086-Activex controls marked safe - Trusted Sit
Rule ID: SV-6342r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI086
Rule Title: The ActiveX controls marked safe for scripting property is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1405 is REG_DWORD=1 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1405 is REG_DWORD=1.

Group ID (Vulid): V-6281
Group Title: DTBI091-Java Permissions not set - Trusted Sites
Rule ID: SV-6348r9_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI091
Rule Title: The Java Permissions is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1C00 is REG_DWORD = 65536, (High Safety), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1C00 is REG_DWORD = 65536, (High Safety).

Group ID (Vulid): V-6282
Group Title: DTBI092-Access data sources across domains-Trusted
Rule ID: SV-6349r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI092
Rule Title: The Access data sources across domains is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Access data sources across domains must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1406 is REG_DWORD=1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1406 is REG_DWORD=1 (Prompt) or 3 (Disabled),.

Group ID (Vulid): V-6283
Group Title: DTBI095-Dont prompt client certificates - Trusted
Rule ID: SV-6350r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI095
Rule Title: The Don't prompt for client certificate selection when no certificate or only one certificate exists is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Client certificates should not be presented to web sites without the user's acknowledgement.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1A04 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2 to the value 1A04 is 3.

Group ID (Vulid): V-6284
Group Title: DTBI097-Installation of desktop items - Trusted Si
Rule ID: SV-6351r7_rule
Severity: CAT II

Rule Version (STIG-ID): DTBI097
Rule Title: The Installation of desktop items is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1800 is REG_DWORD=1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1800 is REG_DWORD=1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6285
Group Title: DTBI098-Launching programs and files in IFRAME-Tru
Rule ID: SV-6352r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI098
Rule Title: The Launching programs and files in IFRAME is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1804 is REG_DWORD=1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1804 is REG_DWORD=1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6286
Group Title: DTBI100-Software channel permissions - Trusted Sit
Rule ID: SV-6353r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI100
Rule Title: The Software channel permissions is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: The Software channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1E05 is REG_DWORD=65536 (High Safety), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1E05 is REG_DWORD=65536 (High Safety).

Group ID (Vulid): V-6287
Group Title: DTBI104-Allow paste operations via script-Trusted
Rule ID: SV-6355r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI104
Rule Title: The Allow paste operations via script is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Allow paste operations via script must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1407 is REG_DWORD=1 (Prompt) or 3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1407 is REG_DWORD=1 (Prompt) or 3 (Disabled).

Group ID (Vulid): V-6288
Group Title: DTBI106-User Authentication - Logon - Trusted Site
Rule ID: SV-6356r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI106
Rule Title: The User Authentication - Logon is not set properly for the Trusted Sites Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1A00 is REG_DWORD=65536 (Prompt), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2

Criteria: If the value 1A00 is REG_DWORD=65536 (Prompt).

Group ID (Vulid): V-6289
Group Title: DTBI112-Download signed ActiveX - Restricted Sites
Rule ID: SV-6357r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI112
Rule Title: The Download signed ActiveX controls property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1001 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1001 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6290
Group Title: DTBI113-Download unsigned ActiveX - Restricted Sit
Rule ID: SV-6358r9_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI113
Rule Title: The Download unsigned ActiveX controls property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls can contain potentially malicious code and must only be allowed to be downloaded from trusted sites and they must be digitally signed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1004 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1004 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6291
Group Title: DTBI114-Initialize and script ActiveX - Restricted
Rule ID: SV-6359r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI114
Rule Title: The Initialize and script ActiveX controls not marked as safe property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1201 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6292
Group Title: DTBI115-Run ActiveX controls and plugins-Restricte
Rule ID: SV-6360r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI115
Rule Title: Run ActiveX controls and plug-ins property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1200 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1200 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6293
Group Title: DTBI116-Script ActiveX controls marked safe-Restri
Rule ID: SV-6361r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI116
Rule Title: The Script ActiveX controls marked safe for scripting property is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: ActiveX controls that are not marked safe for scripting should not be executed. Although this is not a
complete security measure for a control to be marked safe for scripting, if a control is not marked
safe, it should not be initialized and executed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1405 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1405 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6294
Group Title: DTBI119-File download control - Restricted Sites
Rule ID: SV-6362r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI119
Rule Title: The File download control is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Files should not be able to be downloaded from sites that are considered restricted.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1803 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1803 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6295
Group Title: DTBI120-Font download control - Restricted Sites
Rule ID: SV-6363r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI120
Rule Title: The Font download control is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Download of fonts can sometimes contain malicious code. Files should not be downloaded from restricted sites.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1604 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1604 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6297
Group Title: DTBI122-Access data sources - Restricted Sites
Rule ID: SV-6365r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI122
Rule Title: The Access data sources across domains is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: The restricted zones is used for MS Outlook. This zone must be set properly to ensure Outlook is secured.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1406 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1406 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6298
Group Title: DTBI123-Allow META REFRESH - Restricted Sites
Rule ID: SV-6366r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI123
Rule Title: The Allow META REFRESH is not set properly for the Restricted Site Zone.

Vulnerability Discussion: Allow META REFRESH must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1608 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1608 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6299
Group Title: DTBI124-Display mixed content - Restricted Sites
Rule ID: SV-6367r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI124
Rule Title: The Display mixed content is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Mixed content poses a risk when coming from a restricted site.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1609 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1609 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6300
Group Title: DTBI125-Dont prompt client certificate - Restricte
Rule ID: SV-6369r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI125
Rule Title: The Don't prompt for client certificate selection when no certificate or only one certificate exists is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Client certificates should not be presented to web sites without the user's acknowledgement.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1A04 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1A04 is REG_DWORD=3 (Disabled).

Group ID (Vulid): V-6301
Group Title: DTBI126-Drag and drop or copy and paste - Restrict
Rule ID: SV-6370r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI126
Rule Title: The Drag and drop or copy and paste files is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Drag and Drop of files must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1802 is REG_DWORD=3 (Disabled), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1802 is REG_DWORD=3 (Disabled).

Group ID (Vulid): V-6302
Group Title: DTBI127-Installation of desktop items - Restricted
Rule ID: SV-6372r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI127
Rule Title: The Installation of desktop items is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Installation of items must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1800 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1800 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6303
Group Title: DTBI128-Launching programs and files in IFRAME-Res
Rule ID: SV-6373r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI128
Rule Title: The Launching programs and files in IFRAME is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Launching of programs in IFRAME must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1804 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1804 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6304

Group Title: DTBI129-Navigate sub-frames across domain - Restri
Rule ID: SV-6374r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI129
Rule Title: The Navigate sub-frames across different domains is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Frames that navigate across different domains are a security concern because the user may think they are accessing pages on one site while they are actually accessing pages on another site.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1607 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1607 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6305
Group Title: DTBI130-Software channel permissions - Restricted
Rule ID: SV-6375r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI130
Rule Title: The Software channel permissions is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Software channel permissions must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1E05 is REG_DWORD = 65536 (decimal), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1E05 is REG_DWORD = 65536 (decimal).

Group ID (Vulid): V-6306
Group Title: DTBI131-Submit non-encrypted form data-Restricted
Rule ID: SV-6376r9_rule

Severity: CAT II
Rule Version (STIG-ID): DTBI131
Rule Title: The Submit non-encrypted form data is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Submit non-encrypted form data must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security page -> Restricted Sites Zone -> "Submit non-encrypted form data" will be enabled and set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1601 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security page -> Restricted Sites Zone -> "Submit non-encrypted form data" will be enabled and set to “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1601 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6307
Group Title: DTBI132-Userdata persistence - Restricted Sites
Rule ID: SV-6377r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI132
Rule Title: The Userdata persistence is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: No perseistant data should exist and be used in the Restricted sites zone.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1606 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1606 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6308
Group Title: DTBI133-Active scripting - Restricted Sites
Rule ID: SV-6378r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI133
Rule Title: The Active scripting is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Active Scripting must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1400 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1400 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6309
Group Title: DTBI134-Allow paste operations via scripts-Restric
Rule ID: SV-6379r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI134
Rule Title: The Allow paste operations via script is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: The Allow paste operations via script must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1407 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1407 is REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6310
Group Title: DTBI135-Scripting of Java applets - Restricted

Rule ID: SV-6380r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI135
Rule Title: The Scripting of Java applets is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: The Scripting of Java applets must have level of protection based upon the site being accessed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security page -> Restricted Sites Zone -> "Scripting of Java Applets" will be enabled and set to “Disabled”.

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1402 is REG_DWORD = 3 (Disabled = 3), this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security page -> Restricted Sites Zone -> "Scripting of Java Applets" will be enabled and set to “Disabled”. Procedure: Use the Windows Registry Editor to navigate to the following key: HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4 Criteria: Set the value 1402 to REG_DWORD = 3 (Disabled = 3).

Group ID (Vulid): V-6311
Group Title: DTBI136-User Authentication - Logon - Restricted
Rule ID: SV-6381r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI136
Rule Title: The User Authentication – Logon is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Care must be taken with user credentials and how automatic logons are performed and how default Windows credentials are passed to web sites.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1A00 is REG_DWORD = 196608 (decimal), this is not a finding.

Fix Text: Change the registry key HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1A00 is REG_DWORD = 196608 (decimal).

Group ID (Vulid): V-6312
Group Title: DTBI150-Microsoft Java VM is installed
Rule ID: SV-6382r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI150
Rule Title: The Microsoft Java VM is installed.

Vulnerability Discussion: This software is no longer being support and should be removed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Search for the msjava.dll file in the %System root%\System32 by using the Start menu "Search | For Files or Folders…" facility.

Criteria: If the file exists, this is a finding.

Fix Text: Delete the file msjava.dll in the %System root%\System32 by going to the Start menu, Search | For Files or Folders.

Group ID (Vulid): V-6313
Group Title: DTBI151-Cipher setting for DES 56/56 not set
Rule ID: SV-6383r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI151
Rule Title: The Cipher setting for DES 56/56 is not set properly.

Vulnerability Discussion: This cipher setting controls the behavior of the DES 56/56 encryption algorthm.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56

Criteria: If the value Enabled is 0xffffffff, this is not a finding.
The absence of the key also indicates Not a Finding.

Fix Text: Navigate to registry key
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 and change the value to Enabled is 0xffffffff.

Group ID (Vulid): V-6314
Group Title: DTBI152-Cipher setting for Null is not set
Rule ID: SV-6384r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI152

Rule Title: The Cipher setting for Null is not set properly.

Vulnerability Discussion: This controls the behavior of the Null cipher.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL

Criteria: If the value Enabled is 0x0, this is not a finding. The absence of the key also indicates Not a Finding.

Fix Text: Navigate to registry key
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL and change the value to Enabled is 0x0.

Group ID (Vulid): V-6315
Group Title: DTBI153-Cipher setting for Triple DES is not set
Rule ID: SV-6385r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI153
Rule Title: The Cipher setting for Triple DES is not set properly.

Vulnerability Discussion: This enables the Triple Des cipher.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168

Criteria: If the value Enabled is 0xffffffff, this is not a finding. The absence of the key also indicates Not a Finding.

Fix Text: Navigate to the registry key
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168 and change the value to Enabled is 0xffffffff.

Group ID (Vulid): V-6316
Group Title: DTBI160-Hash setting for SHA is not set properly
Rule ID: SV-6386r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI160
Rule Title: The Hash setting for SHA is not set properly.

Vulnerability Discussion: This ensures that the Hash value for SHA is enabled.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA

Criteria: If the value Enabled is 0xffffffff, this is not a finding.

Fix Text: Navigate to the registry key
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA
and change the value to Enabled is 0xffffffff.

Group ID (Vulid): V-6317
Group Title: DTBG007-IE is not capable to use 128-bit encryptio
Rule ID: SV-6387r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTBG007
Rule Title: IE is not capable to use 128-bit encryption.

Vulnerability Discussion: IE must be enabled to use 128 bit encryption. This will lead to stronger encryption when supported by the web server for SSL connections.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: From IE go to the Help | About Internet Explorer dialog. The capability for 128 bit encryption is indicated by the phrase “Cipher Strength: 128 bit.”

Criteria: If the phrase “Cipher Strength: 128 bit” is displayed, this is not a finding.

Fix Text: Install a 128 bit version of IE.

Group ID (Vulid): V-6318
Group Title: DTBG010-DoD Root Certificate is not installed
Rule ID: SV-6388r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTBG010
Rule Title: The DOD Root Certificate is not installed.

Vulnerability Discussion: The DOD root certificate will ensure that the trust chain is established for server certificate issued from the DOD CA.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedures: Open Internet Explorer. From the menu bar select Tools. From the Tools dropdown menu, select the Internet Options. From the Internet Options window, select the Content tab, from the Content tab window select the Publishers… button, from the Publisher window select the Trusted Root Certification Authorities Tab. Scroll through the Certificate Authorities list. Look for the DoD Class 3 Root CA. Click on DoD Class 3 Root CA. Select the View button. From the View Window select the Details Tab

Scroll to the bottom of the Window and select Thumbprint Algorithm in the bottom Pane you should see “sha1”,

Next select Thumbprint

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the Thumbprint Algorithm “sha1” and Thumbprint field is not: DoD Class 3 Root CA certificate is not:
10 f1 93 f3 40 ac 91 d6 de 5f 1e dc 00 62 47 c4 f2 5d 96 71,
then this is a Finding.

Check Content:
Procedure: Use the Tools/Options/Advanced/Encryption dialog. On the Select the View Certificates button. On the Certificate Manager window, select the Authorities tab. Scroll through the Certificate Name list to the U.S. Government heading. Look for the entry for the DoD Class 3 Root CA.
If there is an entry for the DoD Class 3 Root CA, select the entry and then the View button. On the Certificate Viewer window, determine the value of the MD5 Fingerprint field.

Criteria:
If there is no entry for the DoD Class 3 Root CA, then this is a Finding.

If the value of the MD5 Fingerprint field of the DoD Class 3 Root CA certificate is not:
8C:48:08:65:BB:DA:FF:9F:FD:8C:E2:95:E0:96:B9:9D,
then this is a Finding.

If the value of the SHA1 Fingerprint field of the DoD Class 3 Root CA certificate is not:
10:F1:93:F3:40:AC:91:D6:DE:5F:1E:DC:00:62:47:C4:F2:5D:96:71,then this is a Finding.

Fix Text: Install the DOD root certificate.

Group ID (Vulid): V-6319
Group Title: DTBI140-Error Reporting tool is installed or enabl
Rule ID: SV-6389r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI140
Rule Title: The Error Reporting tool for IE is installed or enabled.

Vulnerability Discussion: An error reporting tool may send sensitive data to a vendor.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\ Software\Microsoft\Internet Explorer\Main
and determine the value data for the IEWatsonEnabled value.

Criteria: If the system being reviewed is running Windows XP or 2003, this is not a Finding. [This potential vulnerability is covered in the Windows Checklist.]
If the value data for the IEWatsonEnabled value is not 0 (the number zero) or the key is not found, then this is a Finding.

Fix Text: Navigate to the registry key HKLM\Software\Microsoft\Internet Explorer\Main. Make sure that the key exists and the value data for the IEWatsonEnabled value is 0 (the number zero).

Group ID (Vulid): V-7006
Group Title: DTBI011-IE search parameter is not set correctly.
Rule ID: SV-7341r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI011
Rule Title: The IE search parameter is not set correctly.

Vulnerability Discussion: This parameter ensures automatic searches are not performed from the address bar. When a web site is not found and searching is performed, potentially malicious or unsuited sites may be displayed.

Responsibility: System Administrator
IAControls: ECSC-1

Check Content:
Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Microsoft\Internet Explorer\Main

Criteria: If the value AutoSearch is 0 or 4, this is not a finding.

Fix Text: Use the Windows Registry Editor to navigate to the following key: HKCU\Software\Microsoft\Internet Explorer\Main

Ensure the value AutoSearch is 0 or 4

Group ID (Vulid): V-7007
Group Title: DTBI121-Java Permissions not set for Restricted
Rule ID: SV-7354r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI121
Rule Title: The Java Permissions is not set properly for the Restricted Sites Zone.

Vulnerability Discussion: Java must have level of protection based upon the site being browsed.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1C00 is REG_DWORD = 0 (Disabled = 0), this is not a finding.

Fix Text: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4

Criteria: If the value 1C00 is REG_DWORD = 0 (Disabled = 0).

Group ID (Vulid): V-16879
Group Title: DTBI025 - The Download signed ActiveX controls pro
Rule ID: SV-17879r2_rule
Severity: CAT II
Rule Version (STIG-ID): DTBI025
Rule Title: The Download signed ActiveX controls property is not set properly for the Lockdown Zone.

Vulnerability Discussion: This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded. If you disable the policy setting, signed controls cannot be downloaded. If you do not configure this policy setting, users are queried whether to download controls signed by publishers who aren't trusted. Code signed by trusted publishers is silently downloaded.

Responsibility: System Administrator
IAControls: DCMC-1

Check Content:
The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: If the value 1001 is REG_DWORD = 3, this is not a finding.

Fix Text: The policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Internet Explorer -> Internet Control Panel -> Security Page -> Locked-Down Internet Zone -> "Download signed ActiveX controls" will be set to “Enabled” and "Disable" selected from down drop box.

Procedure: Use the Windows Registry Editor to navigate to the following key:

HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3

Criteria: Set the value 1001 to REG_DWORD = 3.

UNCLASSIFIED